学校编码：10384　　分类号＿＿＿＿　密级＿＿＿＿

学号：X2010230692　　UDC＿＿＿＿

厦门大学

工 程 硕 士 学 位 论 文

税务身份认证系统的设计与实施

Design and Implementation of the Tax Identity Authentication System

石家龙

指 导 教 师： 陈 海 山　教 授

专 业 名 称： 软　件　工　程

论文提交日期： 2012 年 10 月

论文答辩日期： 2012 年 11 月

学位授予日期：　　年　　月

答辩委员会主席：＿＿＿＿＿＿

评　　阅　　人：＿＿＿＿＿＿

2012 年 9 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行)》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名)：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于

年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

金税三期工程是当前税务信息化建设的一次飞越，其主要目标是完成“一个平台，两级处理，三个覆盖，四个系统”的建设。“一个平台”中的网络建设需要有信任体系支撑，信任体系的主要内容包括身份认证、权限管理、责任认定等系统。其中，基于数字证书的身份认证系统是整个网络信任体系的基础。PKI 是基于公开密钥理论和技术建立起来的安全体系，是提供信息安全服务的具有普适性的安全基础设施，是目前解决网络安全问题的最全面的方案。证书认证系统为各行行业提供基础性服务，已在电子政务领域、电子商务领域得到广泛应用。

本文利用成熟的 PKI 技术和证书认证技术，结合税务工作的需要，搭建了一个跨系统的证书认证系统实施平台，为不同的用户提供服务。

本文分析课题研究背景和研究现状，现有的安全机制，阐述 PKI 技术和证书认证技术的相关理论知识，利用 OpenSSL 函数库中的证书和加密函数，在服务器端和客户端分别进行证书设计。结合税务工作的实际，分析系统需求，针对业务范围、用户范围及身份认证和访问控制要求的不同，研究在业务专网上分别建设相对独立的内、外部税务身份认证系统。以税库银系统为例阐述实施过程，说明系统设计及实施的可行性。

关键词：PKI；金税三期工程；身份认证技术

Abstract

Golden-Tax Project III s a flyby in the current tax informatization construction, its main is to achieve "one platform, two stage processing, three cover, four systems" construction. Among them, based on digital certificate of identity authentication system is the foundation of the whole network trust system. PKI is based on public key theory and technology setting up safety system, to provide information security service has universality safety infrastructure, and now to solve the problem of network security is the most complete solution. Certificate authentication system for various industries to provide basic services, has set up a file in the electronic government affairs field, electronic business areas to be widely applied.

This message, by using the mature PKI technology and certificate the authentication technology, combining with the needs of the work of taxation and builting a cross system certificate authentication system implementation platform for different customers.

Based on the analysis of the research background and the present situation, the existing security mechanism, this message expounds PKI technology and certificate authentication technology related theory knowledge, using OpenSSL function library of the certificate and encryption function, in the server and client certificate design respectively. Combined with the actual work of taxation, analysis system requirements, in view of the business scope, user range and identity authentication and access control requirements of the different, research separately in business private network on the relatively independent construction of internal and external tax identity authentication system. To Tax-Treasury-Bank Network for example expounding the implementation, explaining system design and implementation of the feasibility.

Keywords: PKI；The Golden-Tax Project Ⅲ；Identity Authentication Technology

目 录

Contents

第 1 章　绪论

1.1 研究背景及意义

信息化是指在经济和社会活动中，通过大量的采用信息技术、电子装备以及通讯网络等手段，更有效地开发和利用信息资源，使国民经济各部门因信息技术的应用和信息产业的发展而获得巨大利益的过程。税务信息化作为社会信息化的重要组成部分，其含义绝不是模拟手工，其功能也不仅仅是提高效率、节约人力，更重要的是通过其发挥“依托”功能，加强内部监督，杜绝执法随意性，强化外部监控，保障税收执法的刚性，以及提高为纳税人服务的水平等。特别是金税工程三期的上线及试点运行，使得税收信息化从深度到广度都得到了巨大的扩展。

金税三期工程的总体目标是根据一体化原则，建立基于统一规范的应用系统平台，依托计算机网络，总局和省局高度集中处理信息，覆盖所有税种、所有工作环节、国地税机关并与有关部门联网，包括征管业务、行政管理、外部信息、决策支持等四大子系统的功能齐全、协调高效、信息共享、监控严密、安全稳定、保障有力的税收管理信息系统。概括的说，金税三期工程的主要任务就是“一个平台、两级处理、三个覆盖、四个系统”的建设[1]。

所谓“一个平台”，是指建立一个包含网络硬件和基础软件的统一的技术支持平台。即逐步建立覆盖国家税务总局、国地税各级机关、其他政府部门机关及银行系统的网络互联，形成基于因特网的纳税人服务网络平台；对业务处理、在线分析存储系统、数据交换、网络、安全和系统管理七大部分充实配备相应的硬件设备；并建立覆盖从物理环境、网络层、系统层、数据库层、应用层信息安全的安全管理体系和安全技术体系等，以保证税务工作在统一、安全、稳定的网络化平台支撑下平稳运行。而覆盖各级国地税机关、其他政府部门及银行的一个网络系统，对网络的安全性就提出了更高的要求。如何在跨部门、跨系统的网络运行中保障用户及数据资料的安全，就成为了一个极为迫切的问题。

在网络安全方面，金税工程具有其特殊性，因为它的每一条数据的改动都

会引起一系列其他数据表格的联动。所以，保障其网络的安全运行，最主要的即是把握好入口关，即如何做好登录人员的身份确认。

PKI 技术作为信息安全技术的核心，在网络安全中起着至关重要的作用，因此也在当前网络安全环境中被广泛运用。CA 系统（安全认证系统）是 PKI 的核心，是 PKI 不可或缺的部分。但当前的 CA 系统一般只信任自己签发的数字证书或是它信任范围内的数字证书，这对跨部门建立的金税三期网络安全形成很大压力。因此，研究设计基于 PKI 技术的税务身份认证系统就显得尤为重要。

1.2 国内外研究现状

在一些发达国家，PKI 技术已非常成熟，基于 PKI 技术的 CA 身份认证系统也得到了广泛的应用。例如美国为了信息资源的安全共享，以 CA、RA、PMA、CSR 为核心组建了桥接 CA 模式的联邦 FPKI（Federal Public Key Infrastructure）体系, 目的就是为政府部门和其他组织运用数字证书技术来实现信息系统安全、安全电子商务、安全通信等的活动提供设施、规则和政策，支持州及其他地方政府、商业界和大众的安全通信和商务。不仅仅是西方国家，在亚洲，韩国，于 1999 年完成了电子签名法的颁布的执行，并成功建立了 KCAC（Korea Certification & Authentication Central），使其成为本国的根 CA，并在以后的年度内对其进行了修订和完善，为金融、医疗、保险等多个领域公众业务提供 PKI 服务。同样，欧盟也于 2001 年颁布电子签名法后开始启用了欧洲桥 CA，对欧盟各国的电子商务发展起到了极为重要的作用[2]。

我国于 2004 年 8 月 28 日十届人大常委会第十一次会议通过了《中华人民共和国电子签名法》，并于 2005 年开始正式实施。制定本法的目的就是为了规范网络电子签名行为，确立电子签名的法律效力，维护有关网络各方的合法权益。 随着电子商务的快速兴起，我国对于 PKI 技术的研究和运用也得到快速发展。但由于起步较晚，技术尚处于初级运用阶段。现有的基于 PKI 技术的 CA 认证多为政府部门、机关和一些大型商业企业，且各自独立为战，没有统一的根 CA。因此上说，我国的 CA 认证发展任重而道远。

1.3 研究内容及目标

根据我国当前税务工作的现状，结合金税三期工程开展的需求，在税务业务专网上分别建设相对独立的内部和外部税务身份认证系统，以便于分别为税务系统内的税务人员、跨部门系统的其他部门人员及互联网的广大纳税人服务。系统设计以标准化、模块化为原则；各模块之间应相互独立，连接安全，并采用验证机制的安全通信协议；在独立的密码设备中进行安全运算以保证安全性；各内部子系统应有各自独立的数据库且具有访问控制功能。主从发布系统要求处于不同的安全区域。

1.4 本文组织结构

本文共分为六章，各章的主要内容安排如下：

第一章 绪论。主要介绍税务身份认证系统开发的背景及意义，并列述了国内外对身份认证技术的研究及运用现状，表明本文的研究内容和准备达到的预期目标。

第二章 系统相关技术。主要介绍税务身份认证系统所基于的技术，包括 PKI 技术和证书认证技术。

第三章 系统需求分析。主要是对税务身份认证系统的各项需求进行分析，说明系统建设的必要性。

第四章 系统设计。主要介绍了税务身份认证系统设计的思路，列明设计的架构、内部各系统的组成及其功能等。

第五章 系统实施。主要介绍税务身份认证系统平台的应用及基于系统平台税库银的运行实例。

第六章 总结与展望。总结本文所做的主要工作，并针对不足之外提出自己的看法，并指出未来税务身份认证系统的发展方向。

第 2 章　系统相关技术

2.1 PKI 公钥

2.1.1 PKI 的基本概念

公钥基础设施（PKI）是基于公钥理论和技术建立的网络信息安全技术体系，是一种遵循标准的、为用户提供公钥证书管理、密钥管理、网络信息安全应用或安全管理的基础设施。它为网络内实体的认证、证书管理、数字签名、数据加密和网络信息的机密性、真实性、完整性、不可否认性与存取控制等安全需求提供了具有普遍性的基础技术。它属于国家信息安全标准之一。PKI 架构包括网络基础设施、安全支撑平台、应用支撑平台、安全业务应用和系统安全管理等。由于该系统是用公钥密码体制和技术来提供和实施安全服务的基础设施，所以国际上把它叫做公开密钥基础设施（Public Key Infrastructure），简记为 PKI[3]。

公钥基础设施的一般定义为：PKI 是通过使用公开密钥技术和数字证书来确保系统信息安全并负责验证数字证书持有者身份的一种安全基础平台。

学术界定义：PKI 是一种遵循标准的利用非对称密码算法原理来实现并提供安全服务的具有通用性的安全基础设施。

工程专家定义：PKI 是创建、颁发管理、撤销公钥证书所涉及的所有软件、硬件的集合体[4]。

PKI 的核心执行机构是认证机构 CA，PKI 的核心元素是数字证书。PKI 需要与密钥管理基础设施 KMI、权限管理基础设施 PMI 紧密结合，构成安全服务所必需的组件。KMI / PKI / PMI 的体系结构依赖于其支持的应用。公钥基础设施在实际应用中，往往与对称密钥密码算法、数据摘要算法、公钥参数生成算法、随机数生成方法等相结合，共同发挥密码的安全保护作用。

2.1.2 PKI 的主要内容

PKI 首先必须具有可信任的认证机构，在非对称加密技术基础上实现证书的产生、管理、存档、发放以及证书撤销管理等功能，并包括实现这些功能的硬件、软件、人力资源、相关政策和操作规范以及为 PKI 体系中的各成员提供全部的安全服

务等。

构建实施一个 PKI 系统主要包括以下内容：

1、认证机构（CA）

认证机构是 PKI 的核心组成部分，一般简称为 CA，在业界通常称为认证中心。它是数字证书的签发机构[5]。

PKI 服务系统的关键问题是如何实现密钥的管理，公钥机制涉及一对密钥，即公钥和私钥，私钥只能由证书持有者秘密掌握，私钥总是存于发送者和接收者的个人系统中，不能通过公共网络传输；而公钥是公开的，并会在网上进行传输。故公钥的存储、传输、使用是公钥体制中密钥的主要内容之一，目前较好的解决方案是引进证书机制[6]。

证书是公开密钥体制的一种密钥管理媒介，它是数字证书或电子证书的简称，是网上实体身份的证明。证书是由具备权威性、可信任性和公正性的第三方机构（CA）签发的，因此，它是权威性的电子文档。

2、证书库

证书库是 CA 签发证书和已撤销证书列表的集中存放地，它是网络上的一种公共信息库，供公众进行开放式查询。

证书及证书撤销的分发方法是发布，其目的是将 PKI 的信息放在一个广为人知的、公开且容易访问的地点。这对那些大用户群体来说尤其重要，因为这个群体内的人们相互之间都难以认识，这种发布就显得更具有吸引力。到证书库访问查询，可以得到与之通信实体的公钥。证书库是扩展 PKI 系统的一个组成部分，CA 的数字签名保证了证书的合法性和权威性[7]。

3、证书撤销

认证机构 CA 签发证书来为用户的身份和公钥进行捆绑，可是在现实物理世界中，因种种原因，还必须存在一种机制来撤销这种捆绑关系，将现行的证书撤销。这种撤销的原因通常有：用户身份姓名的改变、私钥被窃或泄露、用户与其所属企业关系变更等。这样就必须存在一种方法警告其他用户不要再使用这个公钥。在 PKI 中，这种警告机制被称作证书撤销。所使用的手段为证书撤销列表或称 CRL。

证书撤销的实现方法有两种。一种方法是利用周期性的发布机制，如证书撤销列表 CRL，这是一种常用的方法；另一种方法是在线查询机制，如在线证书状态协